



DEPARTMENT OF THE NAVY  
PERSONNEL SUPPORT ACTIVITY  
937 NORTH HARBOR DRIVE  
SAN DIEGO, CALIFORNIA 92132-0076

PERSUPPACTSANDIEGOINST 5239.2  
N6  
24 Feb 00

**PERSUPPACT SAN DIEGO INSTRUCTION 5239.2**

Subj: USER ACCESS TO NAVY STANDARD INTEGRATED PERSONNEL SYSTEM  
(NSIPS)

Ref: (a) SECNAVINST 5239.3  
(b) OPNAVINST 5239.1B  
(c) CINCPACFLTINST 5239.3  
(d) PERSUPPACTSANDIEGOINST 5239.1D

Encl: (1) NSIPS User Access Request (PSASD Form 5239/1)  
(2) NSIPS Security Accountability Statement

1. Purpose. To establish procedures for, and effectively manage, user access for both Reserve and Active Duty personnel accounts using the Navy Standard Integrated Personnel System (NSIPS) maintained by Personnel Support Activity (PSA) San Diego.

2. Applicability. References (a) through (d) establish requirements for control of user access. This instruction applies to all NSIPS users within the PSA San Diego network.

3. Procedure

a. Each Reserve or Active Duty user needing access to NSIPS must submit, via the assigned supervisor, a completed NSIPS User Access Request Form, enclosure (1), to the Officer in Charge (OIC) of the cognizant Personnel Support Activity Detachment (PSD).

b. The form allows for the following types of requests to be made:

(1) Initial. This form shall be submitted for new users.

(2) Modification. This form shall be submitted for users whose menu access is either increased or decreased.


(3) Deletion. This form shall be submitted whenever users are being transferred, discharged, or separated from the

PERSUPPACT SAN DIEGO INSTRUCTION 5239.2

service. It shall also be used when user access is withdrawn, due to either an administrative or disciplinary reason.

c. The Systems Administrator (SA), serving as the Information Systems Security Officer (ISSO) of the cognizant PSD, is responsible for assigning a USERID on the NSIPS Server and maintaining the security and integrity of user access. Original access request forms, enclosure (1), and accountability statements, enclosure (2), must be filed and tracked, and are subject to review by PSA San Diego's Quality Improvement Visit (QIV) Team.

4. Form. Enclosures (1) and (2) may be reproduced for local use.

  
W. D. ALLISON  
Acting

Distribution:

PERSUPPACTSANDIEGOINST 5216.1I, Lists I and II

# NSIPS USER ACCESS REQUEST

(See instructions on following page)

## PRIVACY ACT STATEMENT

Public Law 99-474, the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, authorizes collection of this information. The information will be used to verify that you are an authorized user of a government automated information system (AIS) and/or to verify your level of government security clearance. Although disclosure of the information is voluntary, failure to provide the information may impede or prevent the processing of your "NSIPS User Access Request." Disclosure of records or the information contained therein may be specifically disclosed outside the DOD according to the "Blanket Routine Uses" set for at the beginning of the DISA compilation of systems of records published annually in the Federal Register, and the disclosures generally permitted under 5 U.S.C. 552a(b) of the privacy act.

### TYPE OF REQUEST:

☐ INITIAL ☐ MODIFY ☐ DELETE

☐ PAY RECORD ACCESS(Active Duty processing only)

1. PSD/RESERVE CENTER UIC:

2. NAME:(Last, First, MI)

3. SOCIAL SECURITY NUMBER:

4. FUNCTION/TITLE:

5. RANK/GRADE:

6. PHONE:

7. TYPE OF RECORDS TO MAINTAIN:

☐ ACTIVE DUTY PERSONNEL

☐ RESERVE PERSONNEL

8. USER ROLE: (Select either a clerk role or supervisor role – a supervisor role inherently assumes 'clerk role' capabilities. The USER ROLE defines the user's menu access.)

### CLERK

☐ PERSONNEL CLERK  
☐ PAY CLERK  
☐ ENTITLEMENT CLERK  
☐ IDT CLERK

### SUPERVISOR

☐ PERSONNEL SUPERVISOR  
☐ PAY SUPERVISOR  
☐ ENTITLEMENT SUPERVISOR  
☐ IDT SUPERVISOR

9. INQUIRY ROLE:

☐ INQUIRY ONLY ACCESS

10. REPORT ROLES: (If user is expected to request reports, then security profile must reflect a "Run Report Role," user inherently receives the view access for reports specifically requested by user. If user requires additional view capabilities, then select applicable "View Report Roles.")

### Run Report Roles

☐ RUN ALL REPORTS(standard and system)  
☐ RUN STANDARD REPORTS

Note: security profile can reflect both roles

### View Report Roles

☐ VIEW SYSTEM REPORTS(run by others)  
☐ VIEW STANDARD REPORTS(run by others)

Note: security profile can reflect both roles

11. WORKFLOW ROLE FOR ROUTING:

☐ ACTIVE CLERK \* ☐ RESERVE CLERK\* or ☐ SUPERVISOR

\*AUDITOR OF TRANSACTIONS SUBMITTED BY CLERK \_\_\_\_\_

(Last,First MI)

Statement of Accountability: I understand my obligation to protect my password. I assume responsibility for data and systems I am granted access to. I will not exceed my authorized access.

12. SIGNATURE OF REQUESTOR:

Verification of need to know: I certify that this user requires access as requested in the performance of his/his job function.

14. SIGNATURE OF SUPERVISOR:

Approval: Access as requested in the performance of his/his job function is approved.

18. SIGNATURE OF OIC:

13. DATE:

15. DATE:  
16. PHONE:

17. ORG/DEPT:

19. DATE:

(To be completed by System Administrator/ISSO only)

COMPLETED BY: \_\_\_\_\_ DATE: \_\_\_\_\_

USER ID ASSIGNED: \_\_\_\_\_ INTERIM PASSWORD ASSIGNED: \_\_\_\_\_

## Instructions for completing NSIPS USER ACCESS REQUEST

**TYPE OF REQUEST:** Check the appropriate type of request.

**PAY RECORD ACCESS:** (*Active duty processing only.*) If the user has pay record access, check this field.

- 1) **PSD/RESERVE CENTER UIC:** The current PSD or Reserve Center UIC of the user.
- 2) **NAME :** The last name, first name and middle initial of the user.
- 3) **SOCIAL SECURITY NUMBER:** The social security number of the user.
- 4) **FUNCTION/TITLE:** The job function of the user (i.e. Pay Clerk, etc.).
- 5) **RANK/GRADE:** The Military rank/rate or the civilian grade of the user (i.e. PNC, E5, LT, GS-7, etc.).
- 6) **PHONE(DSN):** The Defense Switching Network (DSN) phone number of the user. If DSN is unavailable, indicate commercial number including area code.
- 7) **TYPE OF RECORDS TO MAINTAIN:** Place an "X" in the box for the type of records the user will be maintaining. A user, who is responsible for maintaining both Active and SELRES Reserve member data, must be assigned two separate NSIPS signon accounts.
- 8) **USER ROLE:** This is the primary role of the user and determines menu access.
- 9) **INQUIRY ROLE:** This is for users requiring inquiry/read only access.
- 10) **REPORT ROLES:** Report roles are secondary roles. Check the appropriate report role(s), if the user is to run and/or view/print reports.
- 11) **WORKFLOW ROLE FOR ROUTING:** Workflow roles correspond to USER ROLE and determine the automated routing of the events/processes. Example: If the User Role is Pay Clerk and the user maintains active duty personnel records, then the workflow role should be "ACTIVE CLERK." If user has access to active records, then assign Active workflow roles. If user has access to reserve records, then assign Reserve workflow roles.  
\*AUDITOR OF TRANSACTIONS SUBMITTED BY CLERK: This is the person that will be approving transactions submitted by the clerk.
- 12) **SIGNATURE OF REQUESTOR:** Signature of the person requesting access to the system.
- 13) **DATE:** Date the requestor signs the request form.
- 14) **SIGNATURE OF SUPERVISOR:** Signature of the person approving the request.
- 15) **DATE:** Date the supervisor signs the request form.
- 16) **PHONE:** Area code and phone number of supervisor.
- 17) **ORG/DEPT:** Organization or department of supervisor.
- 18) **SIGNATURE OF OIC:** Signature of the OIC approving the request.
- 19) **DATE:** Date the OIC signs the request form.

To be completed by the System Administrator:

**COMPLETED BY:** Printed name and signature of the System Administrator/ISSO setting up the USERID on the NSIPS server.

**DATE:** Print the date the USERID was entered in the system.

**USERID ASSIGNED:** Print assigned USERID.

**INTERIM PASSWORD ASSIGNED:** Print the Interim PASSWORD assigned to the user.

**Note:** USER is to change the password immediately upon receipt of USERID and Interim PASSWORD.

## NSIPS SECURITY ACCOUNTABILITY STATEMENT

### 1. Purpose

The purpose of this document is to inform individuals granted access to NSIPS IT resources of their responsibility to protect those resources from unauthorized use, disclosure, waste, fraud, and abuse.

### 2. Background

The data processed in the NSIPS network are Level II unclassified data. These data, personal and financially sensitive, are protected from unauthorized disclosure and misuse by provisions of the Privacy Act of 1974 and by Public Law 98-473. Individuals disclosing or misusing information obtained from the NSIPS network or using NSIPS equipment for purposes other than those for which it was intended are subject to fines or imprisonment or both. It is incumbent upon individuals granted access to NSIPS IT resources to protect these resources from misuse. The items listed in paragraph 3 of this document, titled Data Security Responsibilities, are items for which authorized users of the NSIPS system are held accountable. To ensure that all authorized users are aware of their responsibilities, this statement of acknowledgement must be executed before permission is granted to use the system and user-ID and password assignments are made.

### 3. Data Security Responsibilities

- a. Protect your individual password from disclosure and use by others. (Do not give to others or post.)
- b. Properly dispose of printed material that contains sensitive financial or Privacy Act information. (Shred or put in burn bag.)
- c. Use NSIPS IT equipment only as intended for authorized purposes. (no games, recipes, bowling scores, etc.)
- d. Do not disclose personal or financial information extracted from the NSIPS system without proper authorization.

### 4. Physical Security Responsibilities

The items in the paragraph are intended to assist all PSD personnel to create and maintain a safe working environment. Security is everyone's responsibility; be alert.

- a. Request identification from an unfamiliar individual in the PSD.
- b. Secure the working spaces when you are the last to leave, when applicable.
- c. Familiarize yourself with fire protection equipment, location, and operation.
- d. Report any suspected security violations to the Information Systems Security Officer (ISSO).
- e. Review and familiarize yourself with the NSIPS security requirements and procedures in the NSIPS Security Manual.
- f. It is prohibited to smoke, eat, or drink beverages while using NSIPS hardware.

### 5. Acknowledgement

I have read, understand, and fully accept the responsibilities outlined in paragraph 3 of this document. I understand that intentional violations of Privacy Act provisions and NSIPS security requirements can lead to disciplinary actions.

---

User Signature

---

ISSO Signature

---

Date